(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 726 676 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
14.08.1996 Bulletin 1996/33

(51) Int. Cl.[6]: **H04N 7/16**

(21) Numéro de dépôt: **96200196.2**

(22) Date de dépôt: **29.01.1996**

(84) Etats contractants désignés:
DE FR GB SE

(30) Priorité: **08.02.1995 FR 9501449**

(71) Demandeurs:
- **PHILIPS ELECTRONIQUE GRAND PUBLIC**
(Sigle: PHILIPS E.G.P.)
92150 Suresnes (FR)
Etats contractants désignés:
FR
- **Philips Electronics N.V.**
5621 BA Eindhoven (NL)
Etats contractants désignés:
DE GB SE

(72) Inventeurs:
- **Le Berre, Jacques**
F-75008 Paris (FR)
- **Persson, Bjorn**
F-75008 Paris (FR)

(74) Mandataire: **Caron, Jean**
Société Civile S.P.I.D.
156, Boulevard Haussmann
75008 Paris (FR)

(54) Procédé de télévision payante

(57) Il est prévu un dispositif de réception maître et au moins un dispositif de réception esclave, munis tous deux d'une carte à puce et destinés à être utilisés dans une même habitation, et le centre de gestion des titres d'accès délivre un message EMM destiné au dispositif de réception maître et protégé par un moyen cryptographique,

- qui ne peut être exploité que par le dispositif de réception maître,
- et qui contient entre autres l'adresse du dispositif de réception maître (A.M) et des données (SL1/EMM,.. , SLn/EMM, ..) concernant les titres d'accès des dispositifs de réception esclaves.

L'utilisateur doit placer dans le dispositif de réception maître une carte à puce esclave, pour que le dispositif de réception maître y inscrive les titres d'accès esclaves.

Applications : télévision à péage.

A.M	Service ref	M / EMM	SL1 / EMM	....	SLn / EMM	Crypto protection

FIG.2

EP 0 726 676 A1

Description

L'invention concerne un procédé de télévision payante basé sur l'emploi chez un usager d'une carte à microprocesseur, dite carte à puce, à insérer dans un organe de décodage/désembrouillage appelé décodeur, procédé dans lequel la carte à puce est utilisée pour stocker, entre autres, des données concernant les titres d'accès de l'usager, ces titres étant chargés par voie hertzienne dans chaque carte à puce d'usager à partir d'un dispositif de gestion central, qui engendre et émet des messages de gestion des titres d'accès.

On appelle titres d'accès un ensemble de données permettant d'établir qu'un usager a le droit de recevoir une émission considérée.

Elle concerne aussi un système de télévision comportant un émetteur et une pluralité d'installations de réception, une installation de réception conçue pour la réception d'émissions payantes possédant au moins un organe de décodage/désembrouillage appelé décodeur, muni d'un lecteur de carte à microprocesseur, dite carte à puce, utilisée pour stocker, entre autres, des données concernant des titres d'accès d'un usager, l'émetteur comprenant un dispositif de gestion qui engendre et émet par voie hertzienne des messages de gestion des titres d'accès.

Elle concerne enfin un dispositif de réception de télévision, muni d'un lecteur pour une carte à microprocesseur, dite carte à puce, dans lequel la carte à puce est utilisée pour stocker, entre autres, des messages de gestion des titres d'accès, émis par un émetteur, protégés par un moyen cryptographique, messages qui ne peuvent être exploités qu'en association avec la carte à puce à laquelle il sont destinés et qui contiennent entre autres un numéro d'identification du dispositif de réception, et des données concernant des titres d'accès, le dispositif de réception étant muni de moyens pour, quand il reçoit un tel message, mettre en oeuvre un processus cryptographique en association avec la carte à puce, c'est-à-dire procéder à l'authentification et au décryptage du message de gestion des titres d'accès et le charger dans sa carte à puce.

Une méthode de contrôle d'accès correspondant au préambule ci-dessus est connue notamment du système EUROCRYPT. La norme concernant ce système (SPECIFICATION DU SYSTEME D2-MAC PAQUETS, édition 1985) décrit, pages 146, 147, un tel procédé d'embrouillage.

Le besoin s'est fait sentir de distribuer à un même usager plusieurs décodeurs, avec leurs cartes à puces associées. L'obtention d'un second ou d'un troisième décodeur par un même usager peut être avantageuse en ce qui concerne le prix d'abonnement pour le second et éventuellement le troisième décodeur, pour lesquels il peut obtenir des réductions.

Il est clair qu'une telle réduction ne peut être accordée que si le second et le troisième décodeurs sont utilisés dans la même maison ou le même appartement. En principe, ce décodeur ne doit pouvoir être donné à des parents ou à des amis.

Un objet de l'invention est de procurer un procédé et un système qui rende difficile l'utilisation d'un décodeur esclave s'il n'est pas utilisé à proximité d'un décodeur maître.

Selon le procédé de l'invention :

- il est prévu en réception un décodeur dit maître et au moins un décodeur dit esclave, devant être utilisés dans une même habitation,
- le dispositif de gestion central délivre un message de gestion des titres d'accès destiné au décodeur maître et qui est exploitable exclusivement par le décodeur maître,
- ce message de gestion des titres d'accès, qui est protégé par un moyen cryptographique, contient entre autres un numéro d'identification du décodeur maître et des données concernant les titres d'accès, y compris ceux d'un décodeur esclave,
- le décodeur maître, quand il reçoit ce message, met en oeuvre un processus cryptographique en association avec la carte à puce, pour procéder à l'authentification et au décryptage du message de gestion des titres d'accès,
- et l'utilisateur place alors dans le décodeur maître une carte à puce esclave, et le décodeur maître y inscrit les titres d'accès esclaves.

L'invention est donc basée sur l'idée d'utiliser le décodeur maître comme boîte aux lettres pour les messages de gestion des titres d'accès destinés aux ensembles décodeur-carte à puce esclaves.

Les titres d'accès destinés au décodeur esclave sont de préférence renouvelés plus souvent que les titres d'accès destinés au décodeur maître, par exemple les titres d'accès destinés au décodeur esclave peuvent être renouvelés au moins chaque semaine alors que les titres d'accès destinés au décodeur maître sont renouvelés tous les mois.

Il y a avantageusement un seul message de gestion des titres d'accès destiné au décodeur maître pour mettre à jour les titres d'accès de plusieurs décodeurs esclaves.

Ainsi le dispositif de gestion ne délivre qu'un message de gestion des titres d'accès pour plusieurs récepteurs, et cela permet de se contenter d'une faible capacité de stockage dans les décodeurs (environ 100 octets).

Un système de télévision payante selon l'invention est remarquable en ce que :

- il comprend dans une même habitation un décodeur dit maître et au moins un décodeur dit esclave, destinés à être utilisés dans cette même habitation,
- le dispositif de gestion est muni de moyens pour délivrer un message de gestion des titres d'accès destiné au décodeur maître, protégé par un moyen cryptographique, message qui est exploitable

exclusivement par le décodeur maître et qui contient entre autres un numéro d'identification du décodeur maître et des données concernant les titres d'accès, y compris ceux d'un décodeur esclave,

- le décodeur maître est muni de moyens pour, quand il reçoit ce message, mettre en oeuvre un processus cryptographique en association avec la carte à puce maître, pour procéder à l'authentification et au décryptage du message de gestion des titres d'accès et le charger dans la carte à puce maître, et de moyens pour inscrire des titres d'accès esclaves dans une carte esclave, lorsqu'une telle carte est placée dans le décodeur maître.

Un dispositif de réception de télévision selon l'invention est avantageusement muni de moyens pour inscrire les titres d'accès d'un décodeur esclave dans une carte à puce esclave, lorsqu'un message de gestion des titres d'accès peut contenir les titres d'accès d'un autre décodeur esclave, associé à une carte esclave.

Ces aspects de l'invention ainsi que d'autres aspects plus détaillés apparaîtront plus clairement grâce à la description suivante d'un mode de réalisation constituant un exemple non limitatif.

La figure 1 représente schématiquement un système selon l'invention.

La figure 2 représente le contenu d'un message de gestion des titres d'accès.

La figure 3 représente schématiquement une installation de réception avec un décodeur maître.

Le système de la figure 1 comprend un centre d'émission ou émetteur 20 et une quantité d'installations de réception dont une est représenté en 21.

Le centre d'émission 20 comprend une source d'images et de son 10, par exemple une caméra de télévision ou un magnétoscope, dont le signal est codé, par exemple en PAL, SECAM, NTSC, etc, ou aussi bien en codage numérique comprimé, dans un codeur 11, puis embrouillé dans une unité d'embrouillage 12, qui ajoute également dans le signal les données d'embrouillage et les éléments cryptographiques nécessaires, fournissant de façon connue aux récepteurs des clés de désembrouillage. Ces données d'embrouillage qui comportent entre autres les titres d'accès, sont engendrées par un dispositif de gestion central des titres d'accès 13.

Le signal est enfin modulé en haute fréquence par un modulateur 14 avant d'être transmis par une antenne d'émission 9, qui peut être aussi une parabole d'émission vers un satellite.

Dans une installation de réception 21, les signaux sont reçus par un organe récepteur, ici une antenne 7, qui pourrait aussi bien être un système de réception satellite ou une antenne collective ou un réseau câblé.

Un répartiteur 8 permet de répartir le signal entre trois installations, par exemple disposées dans trois pièces différentes d'une même habitation, et constituées respectivement d'un téléviseur 4 et d'un décodeur 1 avec une carte à puce 31, d'un téléviseur 5 et d'un décodeur 2 avec une carte à puce 32, d'un téléviseur 6 et d'un décodeur 3 avec une carte à puce 33. Chaque décodeur est relié au téléviseur correspondant par exemple par une connexion de péritélévision standard, permettant le transfert des signaux utiles entre le décodeur et le téléviseur. Un des décodeurs, par exemple le n° 1, est le maître, les deux autres sont esclaves.

Des mécanismes perfectionnés d'adressage et de cryptographie connus en soi sont utilisés pour assurer l'émission et la réception correcte des titres d'accès. Un procédé normalisé, par exemple "Eurocrypt", est utilisable par exemple. Le transport des titres d'accès est fait dans des messages de gestion des titres d'accès, messages dits EMM. Les données contenues dans les titres d'accès sont entre autres des références d'abonnement, des dates de validité, une valeur de crédit, etc.

On enregistre dans le dispositif de gestion 13 les usagers ayant plus d'un ensemble décodeur / carte à puce. L'identification de l'ensemble décodeur / carte à puce maître et de l'ensemble décodeur / carte à puce esclave est donc faite dans le dispositif de gestion : ce dispositif garde trace de tous les ensembles décodeur / carte à puce qui sont distribués aux usagers. Quand un premier ensemble décodeur / carte à puce est fourni à un usager, la clé de distribution de la carte à puce est enregistrée comme maître. Quand un second, puis un troisième ensemble décodeur / carte à puce est fourni au même usager, à la même adresse, la seconde clé de distribution et la troisième clé de distribution sont enregistrées comme esclaves.

Le dispositif de gestion délivre, par exemple une fois par mois, un message EMM pour renouveler les titres d'accès maîtres (un titre d'accès maître est valide un mois). Ce message EMM est reçu par voie hertzienne sur la base du numéro d'identification du décodeur, c'est-à-dire l'adresse du décodeur avec la carte 31, et passé à la carte 31 par le décodeur 1.

Le dispositif de gestion émet, par exemple une fois par semaine, un message EMM destiné au décodeur maître, et contenant en outre les données nécessaires pour chaque carte 32 et 33 afin de renouveler les titres d'accès de ces cartes, qui ne sont alors valables qu'une semaine. Les messages délivrés par le dispositif de gestion ne peuvent être exploités que par le décodeur maître : les titres d'accès esclaves ne sont jamais envoyés directement du dispositif de gestion à l'ensemble décodeur / carte à puce esclave, l'adresse et les données d'authentification qu'ils transportent correspondent au décodeur maître. Ces messages EMM sont stockés dans une mémoire locale du décodeur 1.

Il n'y a pas de différence de matériel (le terme "matériel" est pris ici par opposition au logiciel) entre respectivement un décodeur maître ou une carte à puce maître, et un décodeur esclave ou une carte à puce esclave.

Le contenu du message EMM destiné au décodeur maître, représenté sur la figure 2, contient plusieurs

champs : l'adresse "A.M" du décodeur maître, une référence de service "Service ref", un champ de données pour les titres d'accès maître et esclave "M/EMM", "SL1/EMM",.. , "SLn/EMM", etc, et une donnée de protection cryptographique "crypto-protection". Le champ des titres d'accès peut aussi bien être émis en clair ou crypté.

Quand il reçoit ce message, le décodeur maître met en oeuvre un processus cryptographique connu en association avec la carte à puce, pour l'authentification et la réception des messages EMM, et s'il y a lieu leur décryptage.

L'usager possède ici trois ensembles décodeur / carte à puce chez lui. Il y a donc trois décodeurs 1, 2, 3 et trois cartes à puce 31, 32, 33.

La carte 31 attachée au décodeur 1 est enregistrée au niveau du dispositif de gestion comme carte maître. Les cartes 32, 33 respectivement attachées aux décodeurs 2, 3 sont enregistrées au niveau du dispositif de gestion comme cartes esclaves.

On peut n'avoir qu'un seul message EMM maître pour mettre à jour les titres d'accès des deux décodeurs esclaves. On peut aussi prévoir plusieurs messages, pourvu que chacun soit exploitable exclusivement par le décodeur maître, qui les retransmettra.

Le système peut aussi être simplifié lorsque toutes les cartes esclaves pour un même usager sont des clones, avec la même adresse, les mêmes clés, etc. Bien entendu on peut aussi prévoir des cartes esclaves avec des clés et des adresses différentes.

Une fois par semaine l'usager est obligé d'amener physiquement les cartes 32 et 33 jusque dans le décodeur maître 1, pour mettre à jour les titres d'accès dans les cartes esclaves.

Bien entendu, les durées de validité indiquées ci-dessus sont purement indicatives, toute autre durée peut être choisie.

La réception des titres d'accès ainsi qu'un décodage des signaux d'image et de son sont réalisés chez l'usager par un décodeur. Un décodeur maître 1 est représenté plus en détail sur la figure 3. Il est muni de moyens 16 de réception des émissions hertziennes, d'un module de décodage/désembrouillage 17, et d'un lecteur 18 de carte à puce 31.

Les moyens connus 16 de réception des émissions (syntoniseur, changement de fréquence, amplificateur, démodulateur) envoient au module de décodage/désembrouillage 17 la vidéo et le son embrouillés et des paquets de données. En retour, le module 17 renvoie les signaux désembrouillés qui sont amenés au téléviseur 4.

Le module 17 renvoie de façon connue au dispositif à carte à puce 18-31 certaines des données numériques, notamment des mots de contrôle extraits des dits paquets de données, et la carte fournit en retour un mot d'initialisation qui permet au décodeur de désembrouiller les signaux vidéo. La carte à puce contient une donnée de cryptographie appelée clé de distribution qui est propre à l'usager et qui permet de décrypter les mots de contrôle reçus par voie hertzienne sous forme cryptée, au moyen des susdits mécanismes perfectionnés connus d'adressage et de cryptographie.

Le décodeur lit dans les messages EMM qui lui sont destinés les messages de gestion des titres d'accès pour les décodeurs esclaves. Il les décrypte s'il sont cryptés, au moyen de la clé de distribution de la carte 31. Il les place dans une mémoire 19, dans laquelle il peut les relire pour les entrer dans une carte esclave, que l'usager introduit dans le lecteur 18.

Revendications

1. Procédé de télévision payante basé sur l'emploi chez un usager d'une carte à microprocesseur, dite carte à puce, à insérer dans un organe de décodage/désembrouillage appelé décodeur, procédé dans lequel la carte à puce est utilisée pour stocker, entre autres, des données concernant les titres d'accès de l'usager, ces titres étant chargés par voie hertzienne dans chaque carte à puce d'usager à partir d'un dispositif de gestion central, qui engendre et émet des messages de gestion des titres d'accès, caractérisé en ce que

   - il est prévu en réception un décodeur dit maître et au moins un décodeur dit esclave, devant être utilisés dans une même habitation,
   - le dispositif de gestion central délivre un message de gestion des titres d'accès destiné au décodeur maître et qui est exploitable exclusivement par le décodeur maître,
   - ce message de gestion des titres d'accès, qui est protégé par un moyen cryptographique, contient entre autres un numéro d'identification du décodeur maître et des données concernant les titres d'accès, y compris ceux d'un décodeur esclave,
   - le décodeur maître, quand il reçoit ce message, met en oeuvre un processus cryptographique en association avec la carte à puce, c'est-à-dire procède à l'authentification et au décryptage du message de gestion des titres d'accès,
   - et l'utilisateur place alors dans le décodeur maître une carte à puce esclave, et le décodeur maître y inscrit les titres d'accès esclaves.

2. Procédé selon la revendication 1, caractérisé en ce que les titres d'accès destinés au décodeur esclave sont renouvelés plus souvent que les titres d'accès destinés au décodeur maître.

3. Procédé selon la revendication 2, caractérisé en ce que les titres d'accès destinés au décodeur esclave sont renouvelés au moins une fois par semaine.

4. Procédé selon la revendication 1, caractérisé en ce qu'il y a un seul message de gestion des titres

d'acces destiné au décodeur maître pour mettre à jour les titres d'accès de plusieurs décodeurs esclaves.

5. Système de télévision comportant un émetteur et une pluralité d'installations de réception, une installation de réception conçue pour la réception d'émissions payantes possédant au moins un organe de décodage/désembrouillage appelé décodeur, muni d'un lecteur de carte à microprocesseur, dite carte à puce, utilisée pour stocker, entre autres, des données concernant des titres d'accès d'un usager, l'émetteur comprenant un dispositif de gestion qui engendre et émet par voie hertzienne des messages de gestion des titres d'accès, caractérisé en ce que

   - il comprend dans une même habitation un décodeur dit maître et au moins un décodeur dit esclave, destinés à être utilisés dans cette même habitation,
   - le dispositif de gestion est muni de moyens pour délivrer un message de gestion des titres d'accès destiné au décodeur maître, protégé par un moyen cryptographique, message qui est exploitable exclusivement par le décodeur maître et qui contient entre autres un numéro d'identification du décodeur maître et des données concernant les titres d'accès, y compris ceux d'un décodeur esclave,
   - le décodeur maître est muni de moyens pour, quand il reçoit ce message, mettre en oeuvre un processus cryptographique en association avec la carte à puce maître, c'est-à-dire procéder à l'authentification et au décryptage du message de gestion des titres d'accès et le charger dans la carte à puce maître, et de moyens pour inscrire des titres d'accès esclaves dans une carte esclave, lorsqu'une telle carte est placée dans le décodeur maître.

6. Dispositif de réception de télévision, muni d'un lecteur pour une carte à microprocesseur, dite carte à puce, dans lequel la carte à puce est utilisée pour stocker, entre autres, des messages de gestion des titres d'accès, émis par un émetteur, protégés par un moyen cryptographique, messages qui ne peuvent être exploités qu'en association avec la carte à puce à laquelle il sont destinés et qui contiennent entre autres un numéro d'identification du dispositif de réception, et des données concernant des titres d'accès, le dispositif de réception étant muni de moyens pour, quand il reçoit un tel message, mettre en oeuvre un processus cryptographique en association avec la carte à puce, c'est-à-dire procéder à l'authentification et au décryptage du message de gestion des titres d'accès et le charger dans sa carte à puce, caractérisé en ce que, le message de gestion des titres d'accès pouvant contenir en outre les titres d'accès d'un autre dispositif de réception dit esclave associé à une autre carte à puce dite esclave, le dispositif de réception est muni de moyens pour inscrire les titres d'accès du dispositif de réception esclave dans la carte esclave.

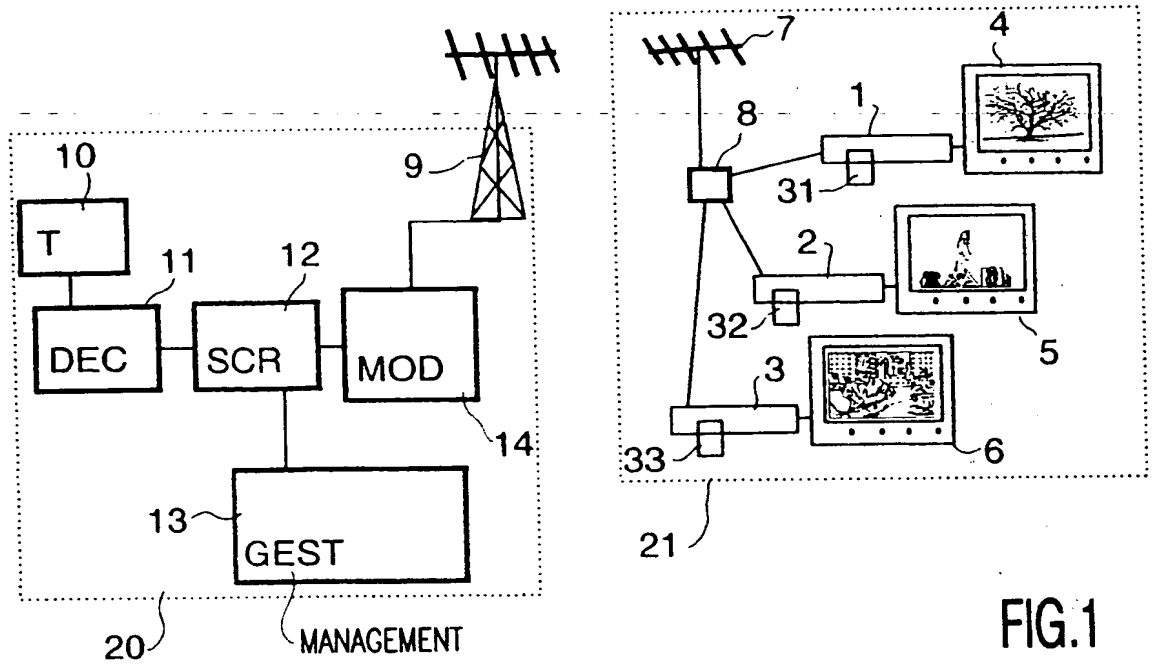

FIG.1

FIG.2

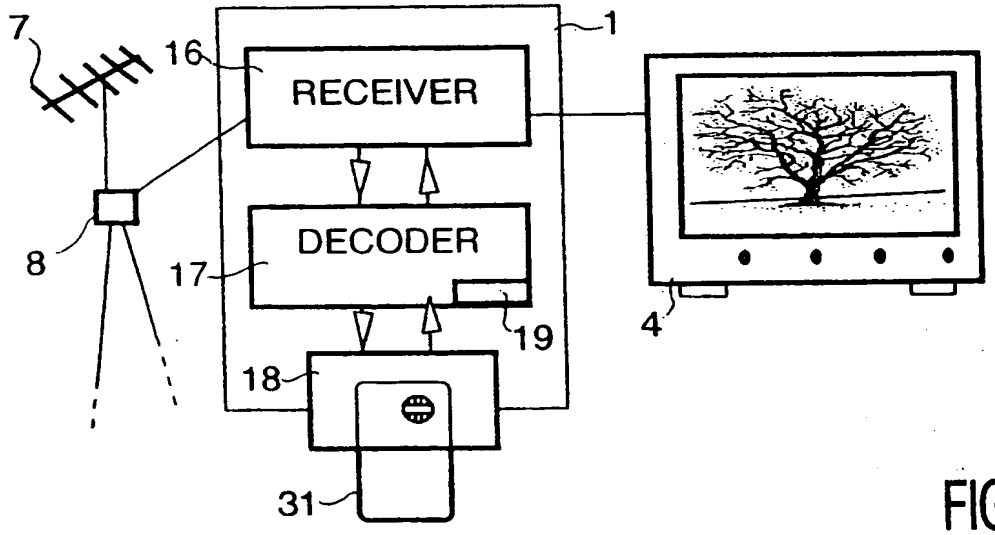

FIG.3

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande
EP 96 20 0196

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.6)
A	FRANK BAYLIN ET AL. 'WORLD SATELLITE TV AND SCRAMBLING METHODS' Septembre 1991 , BAYLIN PUBLICATIONS , BOULDER, CO, US * page 243, colonne de gauche, ligne 35 - page 243, colonne de droite, ligne 40 *	1-6	H04N7/16
A	EP-A-0 570 785 (THOMSON CONSUMER ELECTRONICS) 24 Novembre 1993 * abrégé *	1-6	
A	EP-A-0 489 385 (TECNOENERGIA BY TEL SRL) 10 Juin 1992 * abrégé; figure 1 *	1-6	
A	PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON CONSUMER ELECTRONICS (ICCE), ROSEMONT, JUNE 5 - 7, 1991, no. CONF. 10, 5 Juin 1991 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 206-207, XP 000289007 LENOIR V 'EUROCRYPT, A SUCCESSFULL CONDITIONAL ACCESS SYSTEM' * le document en entier *	1,5,6	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6) H04N
A	FR-A-2 681 165 (GEMPLUS CARD INT.) 12 Mars 1993 * abrégé *	1,5,6	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	2 Avril 1996	Greve, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)